ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №3

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის საქართველოს კანონის მე-7 მუხლის მე-5 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 „გ“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს თანდართული „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტები“.
2. ძალადაკარგულად გამოცხადდეს „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №2 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **დავით ნადირაშვილი**

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისთვის მინიმალური სტანდარტები

მუხლი 1. მიზანი და მოქმედების სფერო

1. ეს სტანდარტები განსაზღვრავს ინფორმაციული უსაფრთხოების მენეჯერის მიმართ არსებულ მოთხოვნებს, მისს უფლება-მოვალეობებსა და ანგარიშვალდებულების წესს.

2. ეს სტანდარტები ვრცელდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად იდენტიფიცირებულ, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებზე (შემდგომ – ორგანიზაცია).

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

მუხლი 2. ინფორმაციული უსაფრთხოების მენეჯერი

ორგანიზაცია ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) მესამე კატეგორიის კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი).

მუხლი 3. ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობები

1. ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობებია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;

ბ) ინფორმაციული უსაფრთხოების მართვის სისტემის მინიმალური მოთხოვნების შესრულების კოორდინირება;

გ) ინფორმაციული აქტივებისა და მათი წვდომის აღწერის ხარისხის უზრუნველყოფა;

დ) ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის (პოლიტიკის, პროცედურების, სახელმძღვანელოების) მომზადების, განხილვის, დამტკიცების და გადახედვის პროცესის კოორდინაცია;

ე) ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვების კოორდინაცია და მათზე რეაგირების მონიტორინგი;

ვ) ინფორმაციული უსაფრთხოების სამოქმედო გეგმის შედგენა და ამ გეგმის შესრულების შესახებ ყოველწლიური ანგარიშის ანგარიშვალდებული პირებისა და საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოსთვის (შემდგომ – სააგენტო) წარდგენა;

ზ) ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობის წარმართვა;

თ) გადაწყვეტილების მიღება სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (CERT.DGA.GOV.GE) მიერ ორგანიზაციის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომის შესაძლებლობის/შეუძლებლობის შესახებ;

ი) ორგანიზაციის თანამშრომლებისთვის ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება;

კ) ინფორმაციული უსაფრთხოების აუდიტის პროცესის ხელშეწყობა.

2. ორგანიზაცია უფლებამოსილია განსაზღვროს ინფორმაციული უსაფრთხოების მენეჯერისთვის სხვა დამატებითი მოვალეობები, რომლებიც ხელს შეუწყობს ორგანიზაციაში ინფორმაციული უსაფრთხოების მოთხოვნების იმპლემენტაციას.

მუხლი 4. ინფორმაციული უსაფრთხოების მენეჯერის ანგარიშვალდებულება

1. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია ორგანიზაციის ხელმძღვანელის ან მის მიერ უფლებამოსილი თანამშრომლის ან ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების უფლებამოსილების მქონე პირთა ჯგუფის (კოლეგიური ორგანოს) წინაშე.

2. ინფორმაციული უსაფრთხოების მენეჯერი ვალდებულია, ყველა მნიშვნელოვანი გადაწყვეტილება, რომლებიც შეეხება ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებას, მიიღოს ანგარიშვალდებულ პირთან/კოლეგიურ ორგანოსთან წინასწარი შეთანხმებით.

მუხლი 5. ინფორმაციული უსაფრთხოების მენეჯერის მიმართ არსებული მოთხოვნები

1. ინფორმაციული უსაფრთხოების მენეჯერის პოზიციის დასაკავებლად პირი უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

ა) ჰქონდეს სულ მცირე 3 წლის სამუშაო გამოცდილება;

ბ) ინფორმაციული უსაფრთხოების დარგში ჰქონდეს შესაბამისი გამოცდის წარმატებით ჩაბარების შედეგად მოპოვებული სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) მოქმედი სერტიფიკატი (წამყვანი დამნერგავი, წამყვანი აუდიტორი ან შიდა აუდიტორი), რომელიც გაცემული იქნება სტანდარტიზაციის ბრიტანული ინსტიტუტის (BSI), ტექნიკური ინსპექტირების ასოციაციის (TÜV) ან პროფესიული შეფასებისა და სერტიფიცირების საბჭოს (PECB) მიერ ან ინფორმაციული უსაფრთხოების დარგში ჰქონდეს შესაბამისი გამოცდის წარმატებით ჩაბარების შედეგად მოპოვებული მოქმედი შემდეგი სერტიფიკატი: CISA/CISM სერტიფიკატი გაცემული ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ, SANS Institute სერტიფიკატი გაცემული GIAC (Global Information Assurance Certification)-ის მიერ ან CISSP (Certified Information Systems Security Professional) სერტიფიკატი გაცემული ინფორმაციული სისტემების უსაფრთხოების სერტიფიცირების საერთაშორისო კონსორციუმის (ISC)² მიერ;

გ) სასურველია ჰქონდეს სამუშაო გამოცდილება ინფორმაციული ტექნოლოგიების, მენეჯმენტის, პროექტების ან/და მართვის სტანდარტების დანერგვის სფეროში.

2. თუ ინფორმაციული უსაფრთხოების მენეჯერს ან კანდიდატს არ გააჩნია ამ მუხლის პირველი პუნქტის „გ“ ქვეპუნქტში აღნიშნული სერტიფიკატებიდან ერთ-ერთი, მან უნდა გაიაროს ამ სტანდარტების მე-6 მუხლის მე-2 პუნქტით გათვალისწინებული ტესტირება.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2022 წლის 10 ოქტომბრის ბრძანება №2 - ვებგვერდი, 10.10.2022 წ.
ციფრული მმართველობის სააგენტოს თავმჯდომარის 2022 წლის 14 ოქტომბრის ბრძანება №3 - ვებგვერდი, 17.10.2022 წ.

მუხლი 6. სააგენტოს მონაწილეობა ინფორმაციული უსაფრთხოების მენეჯერის შერჩევაში

1. ინფორმაციული უსაფრთხოების მენეჯერის პოზიციის მნიშვნელობის, დაკისრებული ამოცანების სირთულისა და კრიტიკულობის გათვალისწინებით, სააგენტო მონაწილეობას იღებს ინფორმაციული უსაფრთხოების მენეჯერის შერჩევის პროცესში.

2. სააგენტოს მონაწილეობა აღნიშნულ პროცესში შემოიფარგლება ინფორმაციული უსაფრთხოების მენეჯერის ან კანდიდატის ინფორმაციული უსაფრთხოების კუთხით ცოდნისა და გამოცდილების, მისი კომპეტენციის ტესტირების საფუძველზე შეფასებაში/დადასტურებაში. სააგენტო ორგანიზაციას ტესტირების თარიღამდე 5 სამუშაო დღით ადრე აცნობებს ტესტირების თარიღს. ტესტირების პასუხები ტესტირებიდან 5 სამუშაო დღეში ეცნობება როგორც ინფორმაციული უსაფრთხოების მენეჯერს/კანდიდატს, ასევე დამსაქმებელ ორგანიზაციას.

3. სააგენტო ინფორმაციული უსაფრთხოების მენეჯერის ან კანდიდატის მიერ ტესტირების წარმატებით გავლის შემთხვევაში, გასცემს სერტიფიკატს 3 წლის მოქმედების ვადით.

4. სააგენტო ტესტირების შედეგებთან ერთად ორგანიზაციას უგზავნის დასკვნას კანდიდატის ინფორმაციული უსაფრთხოების მენეჯერისადმი დადგენილ საკვალიფიკაციო მოთხოვნებთან შესაბამისობის/კანდიდატის ინფორმაციული უსაფრთხოების მენეჯერად დანიშვნის მიზანშეწონილობის შესახებ.