ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №2

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-5 მუხლის მე-4 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 „ბ“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის თანდართული წესები.
2. ძალადაკარგულად გამოცხადდეს „ინფორმაციული აქტივების მართვის წესების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №7 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **დავით ნადირაშვილი**

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესები

მუხლი 1. მიზანი, გავრცელების სფერო

1. ეს წესები ვრცელდება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის (შემდგომ – კანონი) შესაბამისად იდენტიფიცირებულ, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტზე (შემდგომ – სუბიექტი).

2. ეს წესები მიზნად ისახავს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) გავრცელების სფეროში შემავალი ყველა აქტივის მართვას და ითვალისწინებს ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით დამტკიცებულ „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს“ და სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტის – ISO 27000 – განხორციელების საუკეთესო პრაქტიკას.

მუხლი 2. ტერმინთა განმარტება

1. ამ წესებში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) **ინფორმაციული აქტივი** (შემდგომ – აქტივი) – ყველა ინფორმაცია და ცოდნა (ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის.

ბ) **აქტივის მფლობელი** – პირი ან ორგანიზაციული ერთეული, რომელსაც გააჩნია აქტივის შემუშავების, განვითარების, მხარდაჭერის, გამოყენების და დაცვის უფლებამოსილება. მფლობელს არ გააჩნია

აქტივზე რაიმე სახის საკუთრების უფლება;

გ) **უფლებამოსილი ერთეული** – ინდივიდი ან სუბიექტი, რომელსაც გააჩნია აქტივზე წვდომის უფლება;

დ) **ხელმისაწვდომობა** – უფლებამოსილი ერთეულის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი;

ე) **კონფიდენციალურობა** – აქტივის მახასიათებელი, რომლის თანახმადაც აქტივი ხელმისაწვდომია მხოლოდ უფლებამოსილი ერთეულისათვის;

ვ) **მთლიანობა** – აქტივის სიზუსტის და სისრულის მახასიათებელი.

2. ამ წესებში გამოყენებულ სხვა ტერმინებს აქვს კანონით განსაზღვრული მნიშვნელობა.

მუხლი 3. აქტივების მართვა

1. ინფორმაციული აქტივების მართვა გულისხმობს მათი აღწერის, კლასიფიცირების, ხელმისაწვდომობის, გაცემის (გამოქვეყნების), შეცვლისა და განადგურების წესების არსებობას (გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი საჯარო ინფორმაციის ხელმისაწვდომობას განსაზღვრავს).

2. სუბიექტი, საუკეთესო საერთაშორისო პრაქტიკის (მათ შორის, სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტების – ISO 31000; ISO 27005) მხედველობაში მიღების გზითა და ინფორმაციული უსაფრთხოების პოლიტიკის, პროცედურებისა და კონტროლის მექანიზმების გათვალისწინებით, განსაზღვრავს აქტივების მართვის დამატებით წესებს.

მუხლი 4. აქტივების აღწერა

1. სუბიექტი, შინასამსახურებრივი გამოყენების წესების შესაბამისად, ატარებს ინფორმაციული სისტემების ინვენტარიზაციას ყველა ინფორმაციული აქტივის გამოვლენისა და აღრიცხვის მიზნით, რის შედეგადაც ყოველ ინფორმაციულ აქტივს მიენიჭება კრიტიკულობის შესაბამისი კლასი – კონფიდენციალური ან შინასამსახურებრივი გამოყენების. ყველა სხვა ინფორმაციული აქტივი, რომელთა კლასიფიცირება საჭირო არ არის, ღია ინფორმაციად ითვლება. კლასიფიცირებული ინფორმაცია, მისი კლასის შესაბამისად, ექვემდებარება მარკირებას. ყველა ინფორმაციული აქტივი, რომელიც არ არის კლასიფიცირებული კონფიდენციალურ და შინასამსახურებრივი გამოყენების ინფორმაციად, მაინც ექვემდებარება შესაბამის მარკირებას.

2. ინფორმაციული აქტივების აღრიცხვის შედეგად აღიწერება ყოველი ინფორმაციული აქტივის მნიშვნელობა, ფასეულობა, უსაფრთხოებისა და დაცვის არსებული დონე.

3. ინფორმაციული აქტივის შექმნის დროს კრიტიკულობის შესაბამის კლასს ადგენს აქტივის ავტორი ან/და აქტივზე პასუხისმგებელი პირი. ყველა აქტივს უნდა ჰყავდეს აქტივის მფლობელი და განისაზღვროს მისი პასუხისმგებლობები კონტროლის შესაბამის მექანიზმებზე. მფლობელმა შესაძლოა განახორციელოს კონტროლის კონკრეტული მექანიზმების დანერგვის დელეგირება, მაგრამ მფლობელი მაინც რჩება აქტივის სათანადო დაცვაზე პასუხისმგებელ პირად.

4. ინფორმაციული აქტივების მართვის წესები სუბიექტის მიერ უნდა ჩამოყალიბდეს დოკუმენტირებული ფორმით და განხორციელდეს მისი დანერგვა.

5. აქტივების აღწერისას სუბიექტი სარგებლობს ამ წესების №1 დანართში მოცემული ან მის მიერ განსაზღვრული ფორმის შესაბამისად.

მუხლი 5. აქტივების შეფასება

1. სუბიექტი, აქტივების ამ წესების შესაბამისად აღწერის შემდგომ, ვალდებულია, გააანალიზოს რისკები მოცემულ აქტივებთან მიმართებით.

2. სუბიექტის მიერ რისკების ანალიზი და შეფასება უნდა განხორციელდეს „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით დამტკიცებული „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების“ შესაბამისად, და ინფორმაციული უსაფრთხოების რისკების მართვასთან დაკავშირებული საუკეთესო საერთაშორისო პრაქტიკის გათვალისწინებით (სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტები – ISO 31 000, ISO 27005).

მუხლი 6. აქტივების კლასიფიცირება

1. აქტივების კლასიფიცირების მიზანია ინფორმაციის დაცვის სათანადო დონის უზრუნველყოფა.

2. ინფორმაციას გააჩნია სხვადასხვა ხარისხის სენსიტიურობა და კრიტიკულობა, რაც მოითხოვს შესაბამისი დაცვის ხარისხის უზრუნველყოფას ან მოპყრობის გარკვეული წესების არსებობას. ინფორმაციის დაცვის დონე ან/და მოპყრობის საშუალებები განისაზღვრება ინფორმაციის კლასიფიკაციაზე დაყრდნობით, „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად.

მუხლი 7. კლასიფიცირების პროცედურები

1. ინფორმაციის კლასიფიკაცია უნდა მოხდეს „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად, საკანონმდებლო მოთხოვნების, მისი ფასეულობის, კრიტიკულობისა და სენსიტიურობის მხედველობაში მიღების გზით, ასევე გათვალისწინებული უნდა იქნეს უნებართვო გამჟღავნებისა ან ცვლილების შემთხვევები.

2. ინფორმაციის მარკირებისა და მისი მოპყრობის სათანადო პროცედურები დგინდება და ინერგება ორგანიზაციაში მიღებული კლასიფიკაციის სქემის შესაბამისად, „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით დადგენილი წესით.

3. სუბიექტი ახდენს იმ უარყოფითი შედეგების იდენტიფიცირებას, რამაც შეიძლება გამოიწვიოს აქტივების კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა.

4. სუბიექტი ავლენს აქტივებზე კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დარღვევით გამოწვეულ დანაკარგებს და შემდეგ ეტაპზე ატარებს გავლენის შეფასებას, რის შედეგადაც აქტივს მიენიჭება კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შესაბამისი დონე (მაგალითად, მაღალი, საშუალო, დაბალი).

5. უარყოფითი გავლენის ანალიზისთვის საჭირო კრიტერიუმები უნდა შემუშავდეს და განისაზღვროს სუბიექტისთვის მიყენებული სავარაუდო ზიანის ან დანახარჯების მოცულობის გათვალისწინებით. ინფორმაციული უსაფრთხოების ინციდენტმა შესაძლოა გამოიწვიოს უარყოფითი გავლენა, რაც გამოიხატება ინფორმაციული უსაფრთხოების დარღვევაში (კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა), სუბიექტის საქმიანობის და ფინანსური ღირებულების შემცირებაში, გეგმებისა და მათი შესრულების ვადების დარღვევაში, საქმიანი რეპუტაციის შელახვასა ან საკანონმდებლო და სახელშეკრულებო მოთხოვნების დარღვევაში.

6. სუბიექტმა უნდა განსაზღვროს ინციდენტის თითოეული სცენარის გავლენა მის საქმიანობაზე. მან შესაძლოა გავლენა იქონიოს ერთ ან მეტ აქტივზე ან მის ნაწილზე. აქტივებს შესაძლოა დადგენილი ჰქონდეთ ფასეულობა, როგორც ფინანსური თვალსაზრისით, ასევე, ორგანიზაციის საქმიანობისთვის უარყოფითი შედეგების კუთხით.

დანართი №1

აქტივების აღწერის ფორმები კატეგორიების მიხედვით

კატეგორია - ძირითადი ინფორმაცია							
აქტივის №	აღწერა	მფლობელი	ადგილმდებარეობა	მატარებელი/ფორმატი	შექმნის თარიღი	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი

კატეგორია - პროგრამა									
აქტივის №	აღწერა	ბრენდი	სერიული №	აქტივაციის გასაღები	მფლობელი	ადგილმდებარეობა	რეგისტრაციის თარიღი	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი

კატეგორია - კომპიუტერული ტექნიკა								
აქტივის №	აღწერა	ბრენდი ან მოდელი	სერიული №	მფლობელი	ადგილმდებარეობა	რეგისტრაციის თარიღი	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი

კატეგორია - სერვისი								
აქტივის №	აღწერა	მფლობელი (კოორდინატორი)	კომპანია	კონტრაქტი ან კლიენტის №	ძალაში შესვლის თარიღი	ტელ. ნომერი	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი
						(000) 000-0000		

კატეგორია - თანამშრომლები							
თანამდებობის დასახელება/კოდი	სახელი და გვარი	ფუნქცია	სამუშაო ადგილი	დეპარტამენტი	ტელეფონის ნომერი	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი
					(000) 000-0000 / შიდა 0000		

კატეგორია - დოკუმენტი (ელექტრონული ან ქაღალდზე)							
აქტივის №	აღწერა	მფლობელი (კოორდინატორი)	ქვეკატეგორია ელექტრონული /ქაღალდზე	ადგილმდებარეობა (ელექტრონული ან ფიზიკური)	აქტივის ფორმირების თარიღი	აქტივის სტატუსი (არქივი ან წარმოებაში)	კლასიფიკაციის მაჩვენებელი

კატეგორია - შენობა და აპარატურა					
აქტივის №	აღწერა	მფლობელი (კოორდინატორი)	ადგილმდებარეობა	ქვეკატეგორია	კლასიფიკაციის მაჩვენებელი