მონაცემთა გაცვლის სააგენტოს თავმჯდომარის

ბრძანება №7

2013 წლის 7 თებერვალი

ქ. თბილისი

ინფორმაციული აქტივების მართვის წესების 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 ,,ზ“ ქვეპუნქტის თანახმად, **ვბრძანებ**:

მუხლი 1

დამტკიცდეს ,,ინფორმაციული აქტივების მართვის წესები".

მუხლი 2

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

მონაცემთა გაცვლის სააგენტოს თავმჯდომარე **ირაკლი გვენეტაძე**

ინფორმაციული აქტივების მართვის წესები

მუხლი 1. ტერმინთა განმარტება

1. **ინფორმაციული აქტივი (შემდგომში - „აქტივი“)** – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე.
2. **მფლობელი** – „მფლობელი“ არის პირი ან ორგანიზაციული ერთეული, რომელსაც გააჩნია აქტივის შემუშავების, განვითარების, მხარდაჭერის, გამოყენების და დაცვის დადასტურებული მართვის უფლება. „მფლობელი“ არ ნიშნავს, რომ მას გააჩნია აქტივზე რაიმე სახის საკუთრების უფლება.
3. **ავტორიზებული ერთეული** - ინდივიდი, სუბიექტი ან პროცესი, რომელსაც გააჩნია აქტივზე წვდომის უფლება;
4. **ხელმისაწვდომობა** - ავტორიზებული სუბიექტის მოთხოვნის შესაბამისად აქტივზე წვდომის და გამოყენების მახასიათებელი.
5. **კონფიდენციალურობა** - აქტივის მახასიათებელი, რომლის თანახმადაც აქტივი ხელმისაწვდომია მხოლოდ ავტორიზებული ინდივიდების, სუბიექტებისა ან პროცესებისათვის.
6. **მთლიანობა** - აქტივის სიზუსტის და სისრულის მახასიათებელი.

მუხლი 2. მიზანი

1. „ინფორმაციული აქტივების მართვის წესები“ თავსებადია, ერთი მხრივ, საქართველოს კანონთან ,,ინფორმაციული უსაფრთხოების შესახებ“, ხოლო, მეორე მხრივ, იგი ითვალისწინებს და ეფუძნება მგს 27001:2011 „ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნებს“ და ასევე სხვა საუკეთესო პრაქტიკებს.
2. აქტივების მართვის წესების მიზანია განახორციელოს ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომში - „იუმს“) გავრცელების სფეროში გამოვლენილი ყველა აქტივის მართვა. კრიტიკული ინფორმაციული სისტემის სუბიექტმა (შემდგომში - ,,ორგანიზაცია“) უნდა განსაზღვროს კონკრეტულ აქტივზე პასუხისმგებელი პირი ან სტრუქტურული ერთეული.
3. აქტივები წარმოადგენს იუმს-ის საფუძველს, რომლის დანიშნულება არის აქტივების დამცავი და ადექვატური უსაფრთხოების კონტროლის მექანიზმების დანერგვა და დაინტერესებული მხარეების ნდობის გამყარება.
4. აქტივების სრულყოფილი მართვა წარმოადგენს ორგანიზაციაში იუმს-ის დანერგვის და წარმატებული ფუნქციონირების მნიშვნელოვან ფაქტორს. ამასთანავე, აქტივების მართვა განიხილება სხვა მონაცემთა

გაცვლის სააგენტოს თავმჯდომარის ბრძანებით დამტკიცებული „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების“ ერთ-ერთ მოთხოვნად.

მუხლი 3. აქტივების მართვა

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-5 მუხლის მე-4 პუნქტის თანახმად, აქტივების მართვა გულისხმობს შემდეგს: აღწერა, კლასიფიცირება, წვდომა, შეცვლა, განადგურება.

მუხლი 4. აქტივების აღწერა

1. **აქტივების ინვენტარიზაცია** - სავალდებულოა, რომ ყველა აქტივი ზუსტად იყოს გამოვლენილი და აღწერილი.
2. **აქტივების მფლობელის დადგენა** - აქტივს უნდა ჰყავდეს კონკრეტული მფლობელი. უნდა გამოვლინდეს ყველა აქტივის მფლობელი და განისაზღვროს პასუხისმგებლობები კონტროლის შესაბამის მექანიზმებზე. მფლობელებმა შესაძლოა განახორციელონ კონტროლის კონკრეტული მექანიზმების დანერგვის დელეგირება, მაგრამ მფლობელი მაინც რჩება აქტივის სათანადო დაცვაზე პასუხისმგებელ პირად.
3. **აქტივების სათანადო გამოყენება** - ინფორმაციის და ინფორმაციის დამუშავებასთან დაკავშირებული აქტივების მართვის წესები უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და დანერგვა.
4. აქტივების აღწერისთვის ნიმუშის ფორმები წარმოდგენილია დანართი №2-ში.

მუხლი 5. აქტივების შეფასება

1. ორგანიზაციის მიერ აქტივების ზემოთ ჩამოთვლილი ეტაპების მიხედვით აღწერის შემდგომ, მას მოეთხოვება რისკების ანალიზის და შეფასების ჩატარება მოცემულ აქტივებთან მიმართებაში.
2. რისკების ანალიზი და შეფასება ორგანიზაციამ უნდა განახორციელოს „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანების დანართი 1/ა.7.2.1, მე-8 მუხლის მე-4 პუნქტის მიხედვით და ასევე დანართი №1, მგს 27005:2011, მე-8 თავის შესაბამისად.

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 „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანების დანართი 1/ა.7-ის შესაბამისად.
3. საქართველოს კანონი „ინფორმაციული უსაფრთხოების“ შესახებ აწესებს ინფორმაციული აქტივების კრიტიკულობის ორ კლასს: კონფიდენციალური და შინასამსახურებრივი გამოყენების ინფორმაცია.
4. ყველა ინფორმაციული აქტივი, რომელიც არ არის კლასიფიცირებული კონფიდენციალურ და შინასამსახურებრივი გამოყენების ინფორმაციად, მაინც ექვემდებარება შესაბამის მარკირებას.

მუხლი 7. კლასიფიცირების პროცედურები

1. კლასიფიკაციის სახელმძღვანელო - ინფორმაციის კლასიფიცირება უნდა მოხდეს ორგანიზაციაში მისი ღირებულების, საკანონმდებლო მოთხოვნების, სენსიტიურობისა და კრიტიკულობის გათვალისწინებით *(იხ. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანების დანართი 1/ა.7.2.1)*;
2. ინფორმაციის მარკირება და მოპყრობა - ჩამოყალიბდეს და დაინერგოს ინფორმაციის მარკირებისა და მისი მოპყრობის სათანადო პროცედურები ორგანიზაციაში მიღებული კლასიფიკაციის სქემის შესაბამისად *(იხ. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანების დანართი 1/ა.7.2.2*).
3. ორგანიზაციამ უნდა მოახდინოს იმ უარყოფითი შედეგების იდენტიფიცირება, რამაც შეიძლება გამოიწვიოს აქტივების კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა.
4. ორგანიზაციამ უნდა გამოავლინოს აქტივებზე კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დარღვევით გამოწვეული დანაკარგები *(მაგალითისთვის იხ. დანართი 1, მგს 27005:2011, თავი 8.2.1.6.)*. შემდეგ ეტაპზე ჩაატაროს გავლენის შეფასება *(იხ. დანართი 1, მგს 27005:2011, 8.2.2.2.),* რის შედეგადაც აქტივს მიენიჭება კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შესაბამისი დონე (მაგალითად, მაღალი, საშუალო, დაბალი).
5. უარყოფითი გავლენის ანალიზისთვის საჭირო კრიტერიუმები შემუშავებული და განსაზღვრული უნდა იყოს ორგანიზაციისთვის მიყენებული სავარაუდო ზიანის ან დანახარჯების მოცულობის გათვალისწინებით. უარყოფითი გავლენა შესაძლოა გამოწვეული იყოს ინფორმაციული უსაფრთხოების ინციდენტით

(ინციდენტის სცენარი არის საფრთხის მიერ სუსტი წერტილით ან სუსტი წერტილების ნაკრებით სარგებლობის აღწერა ინფორმაციული უსაფრთხოების ინციდენტის დროს) და გავლენა იქონიოს შემდეგზე: ინფორმაციული უსაფრთხოების დარღვევა (მაგალითად: კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვა); ორგანიზაციის საქმიანობის და ფინანსური ღირებულების შემცირება; გეგმებისა და მათი შესრულების ვადების დარღვევა; რეპუტაციის შელახვა; იურიდიული, მარეგულირებელი და სახელშეკრულებო მოთხოვნების დარღვევა.

6. ორგანიზაციამ უნდა განსაზღვროს ინციდენტის თითოეული სცენარის გავლენა ორგანიზაციის საქმიანობაზე. მან შესაძლოა გავლენა იქონიოს ერთ ან მეტ აქტივზე ან მის ნაწილზე. თუმცა აქტივებს შესაძლოა დადგენილი ჰქონდეთ ფასეულობა როგორც ფინანსური თვალსაზრისით, ასევე ორგანიზაციის საქმიანობისთვის უარყოფითი შედეგების კუთხით, თუკი მოხდება მათი დაზიანება ან საფრთხის ქვეშ დაყენება. უარყოფითი შედეგები შესაძლოა იყოს დროებითი ან პერმანენტული, მაგალითად, აქტივის განადგურება.

მუხლი 8. აქტივის მართვის წესები

ორგანიზაცია განსაზღვრავს ინფორმაციული უსაფრთხოების პოლიტიკიდან, პროცედურებიდან და კონტროლის მექანიზმებიდან გამომდინარე აქტივების მართვის წესებს აღნიშნული ბრძანების დანართი №1-ის შესაბამისად.