ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №1

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-4 მუხლის მე-2 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 „ა“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების თანდართული მინიმალური მოთხოვნები.
2. ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №4 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **დავით ნადირაშვილი**

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

თავი I. ზოგადი დებულებები

მუხლი 1. მოქმედების სფერო

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

2. მოთხოვნები ითვალისწინებს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტის (ISO 27000) განხორციელების საუკეთესო პრაქტიკას და მიზნად ისახავს სუბიექტის ინფორმაციული უსაფრთხოების დაცვის ქმედითი და ეფექტიანი განხორციელების მხარდაჭერას.

3. სუბიექტი ვალდებულია მოთხოვნები დანერგოს მისი „პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის დადგენილებით დამტკიცებულ ნუსხაში შეყვანის მომენტიდან 3 (სამი) კალენდარული წლის ვადაში, ამავე მოთხოვნებით გათვალისწინებული წესით.

მუხლი 2. ტერმინთა განმარტება

1. ამ მოთხოვნებსა და მის №1 დანართში გამოყენებულ ტერმინებს აქვთ შემდეგი მნიშვნელობა:

ა) ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები – ინფორმაციული უსაფრთხოების მართვის სისტემის დასანერგად განსაზღვრული საბაზისო მოთხოვნები, რომლებიც სუბიექტმა უნდა

შეასრულოს თანმიმდევრულად;

ბ) ინფორმაციული უსაფრთხოების მართვის სისტემა (შემდგომ – იუმს) – სუბიექტის შიდა (ორგანიზაციული) მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია რისკებისადმი სუბიექტის მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების მოთხოვნების დანერგვა, ფუნქციონირება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

გ) ინფორმაციული აქტივი (შემდგომ – აქტივი) – ყველა ინფორმაცია და ცოდნა (კერძოდ, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ), რომლებიც ღირებულია სუბიექტისათვის;

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

ე) კონფიდენციალურობა – მახასიათებელი, რომლის თანახმად ინფორმაცია სუბიექტის მიერ არ არის გამჟღავნებული ან ხელმისაწვდომი არაუფლებამოსილი ერთეულ(ებ)ისთვის;

ვ) მთლიანობა – ინფორმაციის, ინფორმაციული აქტივის სისწორისა და სისრულის მახასიათებელი;

ზ) ინფორმაციული უსაფრთხოება – ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის შენარჩუნება და დაცვა, რაც დამატებით შესაძლოა მოიცავდეს ისეთ მახასიათებლებს, როგორებიცაა: ავთენტურობა, ანგარიშვალდებულება, წარმოშობის წყაროსთან ცალსახა შესაბამისობა და სანდოობა;

თ) რისკი – ამოცანის შესრულებასთან დაკავშირებული გაურკვევლობის ეფექტი;

ი) რისკის მფლობელი – რისკის მართვაზე ანგარიშვალდებული და უფლებამოსილი პირი ან მისი სტრუქტურული ერთეული;

კ) რეაგირების გარეშე ნარჩენი რისკი – რისკ(ებ)ის მოპყრობის შემდეგ დარჩენილი რისკი;

ლ) რისკის მიღება – სუბიექტის გაცნობიერებული გადაწყვეტილება გარკვეული რისკის მიღების თაობაზე;

მ) რისკის გამოვლენა – რისკის აღმოჩენის, გაცნობიერებისა და აღწერის პროცესი;

ნ) რისკის ანალიზი – რისკის არსის გაცნობიერებისა და რისკის დონის დადგენის პროცესი;

ო) რისკის დონის დადგენა – რისკის ანალიზის შედეგებისა და რისკის კრიტერიუმების შედარების პროცესი, რისკის ან/და მისი სიმძლავრის მისაღებობის ან მის მიმართ ტოლერანტობის დასადგენად;

პ) რისკის მართვა – სუბიექტის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკის გათვალისწინებით;

ჟ) რისკებთან მოპყრობა – რისკის ცვლილების პროცესი;

რ) კონტროლის მექანიზმი – ღონისძიება, რომელიც ცვლის რისკს;

ს) კონტროლის მექანიზმ(ებ)ის გამოყენებადობის განაცხადი – სუბიექტის იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი;

ტ) აუდიტი – ინფორმაციული უსაფრთხოების მართვის სისტემის შემოწმებისთვის მტკიცებულებების მოპოვებისა და მათი ობიექტურად შეფასების სისტემური, დამოუკიდებელი და დოკუმენტირებული პროცესი, რომელიც ადგენს, თუ რამდენად სრულდება შემოწმების კრიტერიუმები;

უ) შინასამსახურებრივი გამოყენების წესები – იუმს-ის ფარგლებში შემუშავებული დოკუმენტაცია (პოლიტიკა, პროცედურები, სახელმძღვანელოები და სხვა ინფორმაციის შემცველი მასალები),

რომელიც ემსახურება კანონის დებულებათა აღსრულებას;

ფ) დაინტერესებული მხარე – ნებისმიერი ფიზიკური ან იურიდიული პირი, ადმინისტრაციული ორგანო, რომელმაც შეიძლება გავლენა მოახდინოს სუბიექტის გადაწყვეტილებასა და ქმედებაზე; აგრეთვე, რომლის ინტერესზეც შესაძლოა გავლენა მოახდინოს სუბიექტის გადაწყვეტილებამ ან ქმედებამ;

ქ) სუბიექტის კრიტიკული ინფორმაციული სისტემა – ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია სუბიექტის ნორმალური ფუნქციონირებისათვის ან/და უზრუნველყოფს სუბიექტის ძირითადი საქმიანობის განხორციელებას.

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

თავი II. სუბიექტის მიერ პირველ წელს შესასრულებელი მოთხოვნები

მუხლი 3. მაღალი რგოლის მენეჯმენტის მხრიდან ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ორგანიზაციული მოწყობა

1. ამ მოთხოვნების გათვალისწინებით სუბიექტმა უნდა ჩამოაყალიბოს, დანერგოს, მხარი დაუჭიროს და მუდმივად გააუმჯობესოს ინფორმაციული უსაფრთხოების მართვის სისტემა.

2. იუმს-თან მიმართებით მაღალი რგოლის მენეჯმენტმა უნდა მოახდინოს ლიდერის როლისა და ნაკისრი ვალდებულების დემონსტრირება, რაც გამოიხატება შემდეგში:

ა) ინფორმაციული უსაფრთხოების პოლიტიკისა და ამოცანების ჩამოყალიბება და სუბიექტის სტრატეგიასთან შესაბამისობის უზრუნველყოფა;

ბ) იუმს-ის მოთხოვნების ინტეგრირება სუბიექტის მიერ განსახორციელებელ პროცესებში;

გ) იუმს-ისთვის საჭირო რესურსების ხელმისაწვდომობა;

დ) ეფექტიანი ინფორმაციული უსაფრთხოებისა და იუმს-ის მოთხოვნების მნიშვნელობის გაცნობიერება;

ე) იუმს-ის მიერ დასახული მიზნ(ებ)ის მიღწევა;

ვ) ჩართულ პირთა ხელმძღვანელობა და მხარდაჭერა, იუმს-ის ეფექტიანობის უზრუნველსაყოფად;

ზ) იუმს-ის მუდმივი გაუმჯობესების ხელშეწყობა;

თ) მენეჯმენტის სხვა წარმომადგენლების მხარდაჭერა, რათა უზრუნველყოფილ იქნეს მათი მხრიდან ლიდერობის გამომჟღავნება საკუთარი პასუხისმგებლობის ფარგლებში.

3. სუბიექტის მაღალი რგოლის მენეჯმენტმა უნდა განსაზღვროს პირი ან პირთა ჯგუფი (რომელიც დაკომპლექტებული იქნება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისაგან), რომელიც განახორციელებს იუმს-ის მხარდაჭერას.

4. მაღალი რგოლის მენეჯმენტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების შესაბამის პირებზე ან პირთა ჯგუფებზე პასუხისმგებლობებისა და უფლებამოსილებების განსაზღვრა და გაცნობა, რათა უზრუნველყოფილი იყოს იუმს-ის:

ა) შესაბამისობა ამ მოთხოვნებთან;

ბ) წარმადობის შესახებ ანგარიშგება მაღალი რგოლის მენეჯმენტთან.

მუხლი 4. იუმს-ის გავრცელების სფეროს განსაზღვრა

1. სუბიექტი ვალდებულია განსაზღვროს ინფორმაციული უსაფრთხოების მართვის სისტემის გავრცელების სფერო და ამ პროცესში გაითვალისწინოს და გამოავლინოს:

ა) ორგანიზაციული კონტექსტი და გარემო ფაქტორები, რომლებიც მნიშვნელოვანია მისი მიზნებისთვის და გავლენას ახდენენ იუმს-ის მიერ დასახული შედეგების მიღწევაზე;

ბ) იუმს-ისთვის მნიშვნელოვანი დაინტერესებული მხარეები, მათი მოთხოვნები და მოლოდინები. დაინტერესებული მხარეების მოთხოვნები შესაძლოა მოიცავდეს როგორც საკანონმდებლო მოთხოვნებს, ასევე სახელშეკრულებო ხასიათის ვალდებულებებს;

გ) სუბიექტის საქმიანობა, ასევე სხვა ორგანიზაციასთან კავშირი და ურთიერთდამოკიდებულება.

2. იუმს-ის გავრცელების სფეროს დადგენისას, სუბიექტმა უნდა განსაზღვროს მასთან არსებული ყველა კრიტიკული ინფორმაციული სისტემა, ინფორმაციული აქტივი, პროცესი, ტექნოლოგია, პროდუქტი/სერვისი, მისი ორგანიზაციული სტრუქტურა და ადგილმდებარეობა, რომლებზეც ვრცელდება იუმს-ისთვის დადგენილი მოთხოვნები.

3. სუბიექტს იუმს-ის გავრცელების სფერო განსაზღვრული უნდა ჰქონდეს მატერიალური/ელექტრონული დოკუმენტის სახით, რომელსაც შეთანხმებისათვის წარუდგენს საჯარო სამართლის იურიდიულ პირს – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო).

მუხლი 5. ინფორმაციული უსაფრთხოების პოლიტიკა

1. სუბიექტის მაღალი რგოლის მენეჯმენტმა უნდა შეიმუშაოს და დაამტკიცოს ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც ეხმიანება სუბიექტის მიზანს და მოიცავს:

ა) ინფორმაციული უსაფრთხოების ამოცანებს ან აყალიბებდეს ინფორმაციული უსაფრთხოების ამოცანების განსაზღვრის ჩარჩოს;

ბ) ინფორმაციულ უსაფრთხოებასთან დაკავშირებული მოთხოვნების შესრულებისთვის ნაკისრ ვალდებულებას;

გ) ინფორმაციული უსაფრთხოების მართვის სისტემის მუდმივი გაუმჯობესებისთვის ნაკისრ ვალდებულებას.

2. სუბიექტის მიერ დამტკიცებული ინფორმაციული უსაფრთხოების პოლიტიკა:

ა) უნდა არსებობდეს დოკუმენტირებული სახით;

ბ) უნდა იყოს ხელმისაწვდომი იუმს-ის გავრცელების სფეროში შემავალი ყველა პირისთვის;

გ) საჭიროების შემთხვევაში, ხელმისაწვდომი უნდა იყოს დაინტერესებული მხარისთვის.

3. ინფორმაციული უსაფრთხოების პოლიტიკის შესაბამისობის, ადეკვატურობისა და ეფექტიანობის უზრუნველყოფის მიზნით, მისი გადახედვა უნდა განხორციელდეს დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებებისას.

მუხლი 6. აქტივების მართვა

სუბიექტმა უნდა განახორციელოს იუმს-ის გავრცელების სფეროში გამოვლენილი აქტივების მართვა, რაც გულისხმობს აქტივების აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და დანერგვას, ამ მოთხოვნების №1 დანართის და „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივების მართვის წესების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად.

მუხლი 7. რისკების შეფასება

1. იუმს-ის დაგეგმვისას სუბიექტმა უნდა გაითვალისწინოს ორგანიზაციული კონტექსტი და გარემო ფაქტორები, დაინტერესებულ მხარეთა მოთხოვნები და მოლოდინები. ასევე, გამოავლინოს რისკები და ახალი შესაძლებლობები, რომლებზეც მოახდენს რეაგირებას, რათა:

ა) უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის საშუალებით დასახული შედეგების მიღწევა;

ბ) თავიდან აიცილოს ან შეამციროს არასასურველი გავლენა;

გ) უზრუნველყოს მუდმივი გაუმჯობესება;

დ) დაგეგმოს საპასუხო ქმედებები და განსაზღვროს მათი ინტეგრაციისა და დანერგვის საშუალებები, აგრეთვე შეაფასოს მათი ეფექტიანობა.

2. სუბიექტმა უნდა განსაზღვროს რისკების შეფასების პროცესი, რომელიც:

ა) აყალიბებს და ხელს უწყობს ინფორმაციული უსაფრთხოების რისკების მიღებისა და შეფასებისთვის საჭირო კრიტერიუმებს;

ბ) უზრუნველყოფს რისკების განმეორებითი შეფასებისას თანმიმდევრული, ვალიდური და შედარებადი შედეგების მიღებას;

გ) რისკის შეფასების პროცესის გამოყენებით გამოავლენს ინფორმაციის კონფიდენციალურობის, მთლიანობის და ხელმისაწვდომობის დაკარგვასთან დაკავშირებულ ინფორმაციული უსაფრთხოების რისკებსა და რისკის მფლობელებს;

დ) აანალიზებს ინფორმაციული უსაფრთხოების რისკებს პოტენციური უარყოფითი შედეგებისა და რისკების ხდომილების ალბათობის ობიექტურად შეფასების გზით;

ე) ადგენს ინფორმაციული უსაფრთხოების რისკების დონეებს რისკების ანალიზის შედეგების შედარებით დადგენილ რისკების კრიტერიუმებთან, რომლის შედეგად გაანალიზებულ რისკებს ენიჭებათ პრიორიტეტები მათი შემდგომი მოპყრობისთვის.

3. სუბიექტმა ინფორმაციული უსაფრთხოების რისკების შეფასების პროცესი უნდა აღწეროს დოკუმენტირებული სახით.

მუხლი 8. რისკებთან მოპყრობა

1. სუბიექტმა უნდა განსაზღვროს და განახორციელოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის პროცესი, რათა:

ა) შეარჩიოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის სათანადო მეთოდები, რისკების შეფასების შედეგების გათვალისწინებით;

ბ) რისკების მოპყრობის შერჩეული მეთოდების დასანერგად გამოავლინოს, საკუთარი მოთხოვნების გათვალისწინებით, თავად შეიმუშაოს ან/და ნებისმიერი წყაროდან შეარჩიოს ყველა საჭირო კონტროლის მექანიზმი;

გ) გამოვლენილი კონტროლის მექანიზმები შეადაროს ამ მოთხოვნების №1 დანართით განსაზღვრულ კონტროლის მექანიზმებს და დარწმუნდეს, რომ ყველა მნიშვნელოვანი კონტროლის მექანიზმი გამოვლენილია. გარდა ამ მოთხოვნების №1 დანართში მითითებულისა, სუბიექტი უფლებამოსილია, თავად განსაზღვროს კონტროლის დამატებითი მიზნები და მექანიზმები;

დ) მოამზადოს კონტროლის მექანიზმების გამოყენებადობის განაცხადი, რომელშიც აღნიშნული იქნება ყველა აუცილებელი კონტროლის მექანიზმი, ასევე მათი შერჩევისა ან გამორიცხვის დასაბუთება

მიუხედავად მათი დანერგვის სტატუსისა;

ე) ჩამოაყალიბოს რისკების მოპყრობის გეგმა;

ვ) უზრუნველყოს რისკების მოპყრობის გეგმის დადასტურება და ნარჩენ რისკებზე თანხმობის მიღება რისკის მფლობელებისგან.

2. სუბიექტმა ინფორმაციული უსაფრთხოების რისკების მოპყრობის პროცესი უნდა აღწეროს დოკუმენტირებული სახით.

3. ამ მოთხოვნების მე-7 და მე-8 მუხლებში აღწერილი რისკების შეფასებისა და მოპყრობის პროცესი თავსებადობაშია ISO 31000-ში მოყვანილ პრინციპებსა და ზოგად სახელმძღვანელო მითითებებთან.

მუხლი 9. ინფორმაციული უსაფრთხოების ამოცანები და მათი შესრულების გეგმები

1. სუბიექტმა უნდა განსაზღვროს ინფორმაციული უსაფრთხოების ამოცანები შესაბამისი ფუნქციებისა და დონეებისთვის. ინფორმაციული უსაფრთხოების ამოცანები:

ა) შესაბამისობაში უნდა იყოს ინფორმაციული უსაფრთხოების პოლიტიკასთან;

ბ) უნდა იყოს გაზომვადი (თუ ეს შესაძლებელია);

გ) უნდა ითვალისწინებდეს ინფორმაციული უსაფრთხოების შესაბამის მოთხოვნებს, ასევე რისკების შეფასების და მათი მოპყრობის შედეგებს;

დ) უნდა არსებობდეს გაცხადებული სახით;

ე) უნდა იყოს განახლებული, საჭიროებისამებრ.

2. ინფორმაციული უსაფრთხოების ამოცანების მიღწევის გზების დაგეგმვისას სუბიექტმა უნდა განსაზღვროს:

ა) გასატარებელი ღონისძიებები;

ბ) საჭირო რესურსები;

გ) პასუხისმგებელი პირ(ებ)ი;

დ) ამოცანის მიღწევის ვადები;

ე) შედეგების შეფასების მეთოდი.

3. სუბიექტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების ამოცანების დოკუმენტირებული სახით არსებობა.

მუხლი 10. იუმს-ის მხარდაჭერა

1. სუბიექტმა უნდა განსაზღვროს და გამოყოს რესურსი იუმს-ის ჩამოყალიბების, დანერგვის, მხარდაჭერისა და მუდმივი გაუმჯობესებისთვის. ამ მიზნით, სუბიექტი ვალდებულია:

ა) განსაზღვროს იუმს-ში შემავალი პირების კომპეტენცია;

ბ) უზრუნველყოს პირების კვალიფიციურობა შესაბამისი ტრენინგებით, სწავლებითა და პრაქტიკული გამოცდილებით;

გ) საჭიროების შემთხვევაში, უზრუნველყოს პირების სათანადო კომპეტენცია (მათ შორის, ტრენინგის ჩატარების, იუმს-ის გავრცელების სფეროში შემავალი პირების სწავლების, ან სამსახურებრივი

პოზიციის ცვლილების, კომპეტენტური პირების დასაქმების ან ხელშეკრულების გაფორმების გზით) და შეაფასოს ამ მიზნით განხორციელებული ქმედებების ეფექტიანობა;

დ) შეინახოს იუმს-ის გავრცელების სფეროში შემავალ პირთა კომპეტენციის დამადასტურებელი დოკუმენტ(ები)ი.

2. იუმს-ის გავრცელების სფეროში შემავალ პირებს უნდა ჰქონდეთ ინფორმაცია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის შესახებ;

ბ) იუმს-ის ეფექტიანობის თვალსაზრისით საკუთარი ფუნქციების, მათ შორის, იუმს-ის მიზნების მიღწევაში შეტანილი წვლილისა და ინფორმაციული უსაფრთხოების წარმადობის შესახებ;

გ) იუმს-ის მოთხოვნების დარღვევით გამოწვეული უარყოფითი შედეგების შესახებ.

3. სუბიექტმა უნდა განსაზღვროს იუმს-ის ფარგლებში შიდა და გარე კომუნიკაციის საჭიროება, აგრეთვე:

ა) კომუნიკაციის საგანი;

ბ) კომუნიკაციის განხორციელების დრო;

გ) კომუნიკაციის წარმმართველი და ადრესატები;

დ) კომუნიკაციის წარსამართად საჭირო სხვა პროცესები.

მუხლი 11. სუბიექტის მიერ იუმს-ის დოკუმენტაციის მართვა

1. იუმს-ის ეფექტიანობის უზრუნველყოფის მიზნით, ის უნდა მოიცავდეს ამ მოთხოვნებით განსაზღვრულ, დოკუმენტირებულ და სუბიექტის მიერ დამატებით განსაზღვრულ სხვა ინფორმაციას.

2. ამ მუხლის პირველ პუნქტში მითითებული ინფორმაციის მოცულობას შესაძლოა განსაზღვრავდეს:

ა) სუბიექტის საქმიანობის ტიპი და მოცულობა, პროცესები, პროდუქტები და მომსახურებები;

ბ) პროცესების სირთულე და მათი ურთიერთქმედება;

გ) იუმს-ის გავრცელების სფეროში შემავალ პირთა კომპეტენცია.

3. დოკუმენტირებული ინფორმაციის შექმნისა და განახლებისას სუბიექტმა უნდა უზრუნველყოს დოკუმენტის:

ა) სათანადო ფორმით იდენტიფიკაცია და აღწერა (სათაური, თარიღი, ავტორი ან საიდენტიფიკაციო ნომერი);

ბ) შესაბამისი ფორმატი (ენა, პროგრამული უზრუნველყოფის ვერსია, გრაფიკული დიზაინი) და მედია-მატარებელი (მატერიალური ან/და ელექტრონული ფორმა);

გ) ადეკვატურობის განხილვა და დამტკიცება.

4. სუბიექტის მიერ იუმს-ის ფარგლებში განსაზღვრულ, დოკუმენტირებულ ინფორმაციაზე უნდა ხორციელდებოდეს კონტროლი, რათა:

ა) საჭიროების შემთხვევაში უზრუნველყოფილ იქნეს მისი ხელმისაწვდომობა და გამოყენებადობა;

ბ) სათანადოდ იყოს დაცული კონფიდენციალურობის დარღვევის, მთლიანობის დაკარგვისა და არასათანადოდ მოხმარებისგან.

5. დოკუმენტირებულ ინფორმაციაზე კონტროლის განხორციელების მიზნით, სუბიექტმა უნდა უზრუნველყოს:

ა) მისი სათანადო გავრცელება, წვდომა, გამოთხოვა და გამოყენება;

ბ) მისი შენახვის წესების დადგენა;

გ) დოკუმენტებში განხორციელებულ ცვლილებათა კონტროლი (ვერსიების კონტროლი);

დ) დოკუმენტების შენარჩუნება და განადგურება.

6. სუბიექტის მიერ უნდა ხორციელდებოდეს იუმს-ის დაგეგმვისა და ფუნქციონირებისთვის საჭიროდ მიჩნეული, გარე წყაროდან მიღებული, დოკუმენტირებული ინფორმაციის იდენტიფიცირება და მის გამოყენებაზე კონტროლი.

თავი III. სუბიექტის მიერ მეორე წელს შესასრულებელი მოთხოვნები

მუხლი 12. ინფორმაციულ უსაფრთხოებასთან დაკავშირებული პროცესების, გეგმების და ამოცანების აღსრულება

1. პირველ წელს შესასრულებელი მოთხოვნების დაკმაყოფილების შემდეგ, მეორე წელს სუბიექტი ვალდებულია:

ა) დაგეგმოს, დანერგოს და აკონტროლოს ინფორმაციული უსაფრთხოების მოთხოვნების დაკმაყოფილების პროცესი და გაატაროს ამ მოთხოვნების მე-7 და მე-8 მუხლებით განსაზღვრული ღონისძიებები;

ბ) განახორციელოს ამ მოთხოვნების მე-9 მუხლით განსაზღვრული გეგმები ინფორმაციული უსაფრთხოების ამოცანების შესასრულებლად;

გ) პროცესების გეგმის მიხედვით შესრულებასთან დაკავშირებით შეინახოს დოკუმენტირებული ინფორმაცია;

დ) აკონტროლოს დაგეგმილი ცვლილებები, განიხილოს გაუთვალისწინებელი ცვლილებებით გამოწვეული უარყოფითი შედეგები და საჭიროებისამებრ, მოახდინოს მათზე რეაგირება უარყოფითი გავლენის შესამცირებლად;

ე) გამოავლინოს მესამე მხარის მიერ განხორციელებული მომსახურება და უზრუნველყოს მათზე კონტროლი.

2. სუბიექტმა უნდა შეაფასოს ინფორმაციული უსაფრთხოების რისკები დაგეგმილი პერიოდულობით ან მნიშვნელოვანი ცვლილებების შემთხვევაში, ამ მოთხოვნების მე-7 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით დადგენილი კრიტერიუმების გათვალისწინებით. სუბიექტმა უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების რისკის შეფასების შედეგების დოკუმენტირებული ფორმით არსებობა.

3. სუბიექტი ვალდებულია დანერგოს ინფორმაციული უსაფრთხოების რისკების მოპყრობის გეგმა და უზრუნველყოს ინფორმაციული უსაფრთხოების რისკებთან მოპყრობის შედეგების დოკუმენტირებული ფორმით არსებობა.

მუხლი 13. სუბიექტის მიერ კონტროლის მექანიზმების დანერგვა

ინფორმაციული უსაფრთხოების მიზნების მისაღწევად სუბიექტი ვალდებულია:

ა) დანერგოს ამ მოთხოვნების მე-8 მუხლის პირველი პუნქტის „დ“ ქვეპუნქტის შესაბამისად შერჩეული კონტროლის მექანიზმები;

ბ) კონტროლის მექანიზმების დანერგვისთანავე აწარმოოს მათზე დაკვირვება;

გ) გააანალიზოს დაკვირვების შედეგები და, საჭიროების შემთხვევაში, განსაზღვროს გაუმჯობესების გზები.

თავი IV. სუბიექტის მიერ მესამე წელს შესასრულებელი მოთხოვნები

მუხლი 14. ინფორმაციული უსაფრთხოების წარმადობისა და იუმს-ის ეფექტიანობის შეფასებისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა

1. ინფორმაციული უსაფრთხოების წარმადობისა და იუმს-ის ეფექტიანობის შეფასების მიზნით, სუბიექტმა უნდა განსაზღვროს:

ა) მონიტორინგის და შეფასების საგანი, მათ შორის, ინფორმაციული უსაფრთხოების პროცესები და კონტროლის მექანიზმები;

ბ) ვალიდური შედეგების მისაღწევად საჭირო მონიტორინგის, ანალიზისა და შეფასების ისეთი მეთოდები, რომლებიც უზრუნველყოფს შედარებადი და განმეორებადი შედეგის მიღწევას;

გ) მონიტორინგის და გაზომვის განხორციელების დრო;

დ) მონიტორინგისა და გაზომვის განმახორციელებელი პირ(ებ)ი;

ე) მონიტორინგის და გაზომვების შედეგების გაანალიზებისა და შეფასების დრო;

ვ) შედეგების გაანალიზებასა და შეფასებაზე პასუხისმგებელი პირ(ებ)ი.

2. სუბიექტმა უნდა უზრუნველყოს მონიტორინგისა და შეფასების შედეგების დოკუმენტირებული ფორმით არსებობა.

მუხლი 15. იუმს-ის შიდა აუდიტი

1. სუბიექტი ვალდებულია ჩაატაროს შიდა აუდიტი დაგეგმილი პერიოდულობით, ინფორმაციული უსაფრთხოების მართვის სისტემის თაობაზე შემდეგი ინფორმაციის მისაღებად:

ა) იუმს-ის სუბიექტის მიერ განსაზღვრულ მოთხოვნებთან შესაბამისობა;

ბ) იუმს-ის ამ მოთხოვნებთან შესაბამისობა;

გ) იუმს-ის ეფექტიანად დანერგვა და მისი მხარდაჭერა.

2. ამ მუხლის პირველი პუნქტით გათვალისწინებული ვალდებულების გარდა, სუბიექტი აგრეთვე, ვალდებულია:

ა) დაგეგმოს, ჩამოაყალიბოს, დანერგოს და მართოს აუდიტის პროგრამა/პროგრამები, რაც გულისხმობს აუდიტის ჩატარების სიხშირის, მეთოდების, პასუხისმგებლობების, დაგეგმვის მოთხოვნების განსაზღვრასა და ანგარიშგებას. აუდიტის პროგრამაში/პროგრამებში გათვალისწინებული უნდა იყოს აუდიტის გავრცელების სფეროში შემავალი პროცესების მნიშვნელობა და წინა აუდიტის შედეგები;

ბ) დაადგინოს აუდიტის კრიტერიუმები და აუდიტის ფარგლები თითოეული აუდიტისთვის;

გ) შეარჩიოს აუდიტორები და ჩაატაროს აუდიტი ობიექტურად და მიუკერძოებლად;

დ) უზრუნველყოს აუდიტის შედეგების შესაბამისი ხელმძღვანელი პირების მიერ განხილვა;

ე) შეინახოს აუდიტის პროგრამ(ებ)ისა და აუდიტის შედეგების დოკუმენტირებული ინფორმაცია.

3. შიდა აუდიტი ტარდება სუბიექტის ან მესამე პირის მიერ სუბიექტის სახელით.

მუხლი 16. ხელმძღვანელობის მიერ იუმს-ის განხილვა

1. სუბიექტის მაღალი რგოლის მენეჯმენტმა დაგეგმილი პერიოდულობით უნდა განიხილოს იუმს-ი, რათა უზრუნველყოფილ იქნეს მისი მუდმივი შესაბამისობა, ადეკვატურობა და ეფექტიანობა. განხილვისას გათვალისწინებული უნდა იქნეს შემდეგი საკითხები:

ა) წინა განხილვის შემდგომ განხორციელებულ ღონისძიებათა სტატუსი;

ბ) ორგანიზაციული კონტექსტის და გარე ფაქტორების ცვლილებები, რომლებმაც შესაძლოა გავლენა იქონიონ ინფორმაციული უსაფრთხოების მართვის სისტემაზე;

გ) უკუკავშირი ინფორმაციული უსაფრთხოების წარმადობასთან დაკავშირებით, მათ შორის:

გ.ა) შეუსაბამობები და მაკორექტირებელი ქმედებები;

გ.ბ) მონიტორინგისა და გაზომვის შედეგები;

გ.გ) აუდიტის შედეგები;

გ.დ) ინფორმაციული უსაფრთხოების ამოცანების შესრულება.

დ) უკუკავშირი დაინტერესებული მხარეებისგან;

ე) რისკების შეფასების შედეგები და რისკებთან მოპყრობის გეგმის სტატუსი;

ვ) ახალი შესაძლებლობები გაუმჯობესებისთვის.

2. სუბიექტის მაღალი რგოლის მენეჯმენტის მხრიდან მუდმივი გაუმჯობესების შესაძლებლობებისა და მართვის სისტემის ცვლილებების საჭიროებების შესახებ განხილვის შედეგები უნდა აისახოს შესაბამისი გადაწყვეტილების ფორმით.

მუხლი 17. შეუსაბამობა და მაკორექტირებელი ქმედებები

1. აუდიტის შედეგად აღმოჩენილი შეუსაბამობის არსებობის შემთხვევაში სუბიექტი ვალდებულია:

ა) მოახდინოს მასზე რეაგირება, და შესაბამისად:

ა.ა) განახორციელოს ქმედებები შეუსაბამობის კორექტირებისთვის;

ა.ბ) გაუმკლავდეს და დაძლიოს შეუსაბამობით გამოწვეული უარყოფითი შედეგები;

ბ) შეაფასოს იმ ქმედებების საჭიროება, რომელთა მეშვეობითაც აღმოიფხვრება შეუსაბამობის მიზეზები მათი განმეორების თავიდან აცილების მიზნით. ამისათვის სუბიექტი ვალდებულია:

ბ.ა) განიხილოს შეუსაბამობა;

ბ.ბ) გამოავლინოს შეუსაბამობის მიზეზები;

ბ.გ) გამოავლინოს მსგავსი შეუსაბამობები ან მათი პოტენციური არსებობის შესაძლებლობა;

გ) შეფასების შედეგების საფუძველზე, შეუსაბამობების განმეორების თავიდან აცილების მიზნით, განახორციელოს საჭირო ქმედება;

დ) განიხილოს უკვე გატარებული მაკორექტირებელი ქმედებების ეფექტიანობა;

ე) საჭიროების შემთხვევაში განახორციელოს ცვლილებები ინფორმაციული უსაფრთხოების მართვის სისტემაში.

2. მაკორექტირებელი ქმედებები უნდა იყოს შეუსაბამობის გავლენის პროპორციული.

3. სუბიექტი ვალდებულია უზრუნველყოს დოკუმენტირებული ინფორმაციის არსებობა, რომლითაც დასტურდება:

ა) შეუსაბამობების ხასიათი და განხორციელებული ქმედებები;

ბ) გატარებული მაკორექტირებელი ქმედებების შედეგები.

მუხლი 18. მუდმივი გაუმჯობესება

სუბიექტმა მუდმივად უნდა გააუმჯობესოს ინფორმაციული უსაფრთხოების მართვის სისტემის შესაბამისობა, ადეკვატურობა და ეფექტიანობა.