ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №4

2020 წლის 16 ოქტომბერი

ქ. თბილისი

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, მე-13 მუხლის პირველი და მე-7 პუნქტებისა და „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლის შესაბამისად, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები.

მუხლი 2

ძალადაკარგულად გამოცხადდეს „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №2 ბრძანება.

მუხლი 3

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **გიორგი მეჟლუმიანი**

ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები

თავი I
ზოგადი დებულებები

მუხლი 1. შესავალი

1. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები (შემდგომ – მოთხოვნები) სავალდებულოა შესასრულებლად „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის პირველი პუნქტის თანახმად იდენტიფიცირებული კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის (შემდგომ – ორგანიზაცია).

2. ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები თავსებადობაშია, ერთი მხრივ, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონთან, ხოლო, მეორე მხრივ, შეესაბამება ISO 27000 სტანდარტის განხორციელების საუკეთესო პრაქტიკას.

მუხლი 2. ტერმინები და განმარტებები

1. ამ მოთხოვნებში გამოყენებული ტერმინები განიმარტება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით დადგენილი შინაარსით და გამოიყენება როგორც კანონით დადგენილი ტერმინების დამატებითი და დამაზუსტებელი განმარტებები.

2. ამ მოთხოვნებში გამოყენებულ ტერმინებს ამ ბრძნების მიზნებისთვის აქვს შემდეგი მნიშვნელობა:

ა) **ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები** – საბაზისო მოთხოვნები, რომლებიც ორგანიზაციამ უნდა შეასრულოს თანმიმდევრულად 3 წლის ვადაში ინფორმაციული უსაფრთხოების მართვის სისტემის დასანერგად;

ბ) **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 კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე;

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

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

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

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

ზ) **ინფორმაციული უსაფრთხოება** – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას;

თ) **ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს)** – მართვის სისტემის ნაწილი, რომელიც დაფუძნებულია ბიზნესის რისკებისადმი მიდგომაზე, რათა შესაძლებელი გახდეს ინფორმაციული უსაფრთხოების დანერგვა, ფუნქციონერება, მონიტორინგი, განხილვა, მხარდაჭერა და გაუმჯობესება;

ი) **რეაგირების გარეშე ნარჩენი რისკი** – რისკების მოპყრობის შემდეგ დარჩენილი რისკი;

კ) **რისკის მიღება** – გადაწყვეტილება რისკის მიღების თაობაზე;

ლ) **რისკის ანალიზი** – ინფორმაციის სისტემური გამოყენება რისკის წარმოშობის წყაროსა და მისი შეფასების დასადგენად;

მ) **რისკის დონის დადგენა** – რისკის მნიშვნელოვნების დასადგენად რისკის მიახლოებითი შეფასების შედეგების შედარება მოცემულ რისკის კრიტერიუმებთან;

ნ) **რისკების მართვა** – ორგანიზაციის მართვისა და კონტროლისათვის საჭირო კოორდინირებული ქმედებების განხორციელება რისკების გათვალისწინებით;

ო) **რისკების მოპყრობა** – რისკის შეცვლისათვის შეფასების საზომების შერჩევისა და მათი დანერგვის პროცესი;

პ) **კონტროლის მექანიზმების გამოყენებადობის განაცხადი** – ორგანიზაციის იუმს-ისთვის გამოსადეგი და გამოყენებადი კონტროლის მიზნებისა და კონტროლის მექანიზმების დოკუმენტირებული განაცხადი.

თავი II

ორგანიზაციისთვის პირველ წელს შესასრულებელი მოთხოვნები

მუხლი 3. ორგანიზაციაში ინფორმაციული უსაფრთხოების აუცილებლობის გაცნობიერება და ხელმძღვანელობის მხრიდან მხარდაჭერა

ორგანიზაციაში უნდა არსებობდეს შინასამსახურებრივი დოკუმენტი ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის შესახებ *(იხ. დანართი № 1, ცმს 27001:2011, თავი 5.1 და 5.2; აგრეთვე დანართი ა-დან კონტროლი ა.6.1.1.)*.

მუხლი 4. ორგანიზაციული მოწყობა

ორგანიზაციამ უნდა განსაზღვროს პირი ან პირები (მაგალითად, ინფორმაციული უსაფრთხოების საბჭო, რომელიც შედგება ინფორმაციული უსაფრთხოების მენეჯერისა და საკვანძო, დარგობრივი ან მიმართულებების ხელმძღვანელი პირებისაგან), რომელიც განახორციელებს ინფორმაციული უსაფრთხოების მართვას *(იხ. დანართი № 1, ცმს 27001:2011, თავი 5.1; კონტროლები: ა.6.1.1; ა.6.1.2; ა. 6.1.3.*“).

მუხლი 5. გავრცელების სფერო

ორგანიზაციამ უნდა განსაზღვროს და დოკუმენტირებულად წარმოადგინოს იუმს-ის გავრცელების სფერო და საზღვრები საქმიანობის, ორგანიზაციული სტრუქტურის, ადგილმდებარეობის, აქტივებისა და ტექნოლოგიების ჭრილში, მათ შორის, დაასაბუთოს დაშვებული გამონაკლისების მიზეზები და შეათანხმოს ისინი საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედ საჯარო სამართლის იურიდიულ პირთან - ციფრული მმართველობის სააგენტოსთან (შემდგომ – სააგენტო) (იხ. *დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ა*).

მუხლი 6. იუმს-ის პოლიტიკა

1. ორგანიზაციამ უნდა წარმოადგინოს ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) პოლიტიკის დოკუმენტი, რომელშიც ასახული იქნება ორგანიზაციის მიერ ინფორმაციული უსაფრთხოების მართვის სისტემის ხედვა, დასახული მიზნები და სასურველი შედეგები და დამტკიცებული იქნება ხელმძღვანელობის მიერ *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ბ-5*).

2. ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემა უნდა უზრუნველყოფდეს დაგეგმვის, დანერგვის, ფუნქციონირების, მონიტორინგისა და გაუმჯობესებისთვის საჭირო ფაზებს *(იხ. დანართი № 1, ცმს 27001:2011, თავები: 4.1; 4.3.1ა,ბ,გ; კონტროლები: ა.5.1.1; ა.5.1.2*“).

3. ინფორმაციული უსაფრთხოების პოლიტიკა:

ა) შეიცავს ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემის მიზანს, ძირითად მიმართულებას და პრინციპებს *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ბ-1*);

ბ) ითვალისწინებს განაცხადს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის და სხვა სტანდარტების მოთხოვნებთან შესაბამისობის შესახებ *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ბ-2; კონტროლი ა. 15.1*);

გ) პასუხობს ორგანიზაციის რისკების მართვის კონტექსტს, რომლის ფარგლებშიც მოხდება იუმს-ის ჩამოყალიბება და მხარდაჭერა *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ბ-3*).

მუხლი 7. აქტივების მართვა

1. ორგანიზაციამ უნდა განახორციელოს დადგენილ გავრცელების სფეროში გამოვლენილი აქტივების მართვა, რაც გულისხმობს აქტივების აღწერის, კლასიფიცირების, შეცვლისა და განადგურების წესების შემუშავებასა და უზრუნველყოფას *(ასევე, იხ. დანართი № 1, ცმს 27001:2011, კონტროლები: ა.7.1 და ა.7.2 სრულად*).

2. ორგანიზაციამ აქტივების მართვა უნდა განახორციელოს სააგენტოს თავმჯდომარის მიერ დამტკიცებული „ინფორმაციული აქტივების მართვის წესების“ შესაბამისად.

მუხლი 8. რისკების მართვა

1. ორგანიზაციამ უნდა განსაზღვროს რისკების შეფასების მიდგომა *(იხ. დანართი № 1, ცმს 27001:2011,*

თავი 4.2.1.გ);

2. ორგანიზაციამ უნდა გამოავლინოს რისკები და გაანალიზოს მათი გავლენა *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.დ);*

3. ორგანიზაციამ უნდა ჩაატაროს გამოვლენილი რისკების ანალიზი და შეფასება *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ე);*

4. ორგანიზაციამ უნდა გამოავლინოს და შეაფასოს რისკების მოპყრობის გზები *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ვ);*

5. ორგანიზაციამ რისკების მოპყრობის მიზნით უნდა შეარჩიოს კონტროლის მიზნები და კონტროლის მექანიზმები *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.ზ);*

6. ორგანიზაციის ხელმძღვანელობამ უნდა დაადასტუროს ნარჩენ რისკებზე თანხმობა *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.თ).*

მუხლი 9. კონტროლის მექანიზმების გამოყენებადობის განაცხადი

ორგანიზაციამ უნდა მოამზადოს კონტროლის მექანიზმების გამოყენებადობის განაცხადი (იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.1.კ), რომელიც შეიცავს:

ა) ამ მოთხოვნების მე-8 მუხლის მე-5 პუნქტში შერჩეულ კონტროლის მიზნებს და კონტროლის მექანიზმებს, ასევე, მათი შერჩევის დასაბუთებას;

ბ) ორგანიზაციაში უკვე დანერგილ კონტროლის მიზნებს და კონტროლის მექანიზმებს;

გ) ცმს 27001:2011-ის დანართი ა-დან ნებისმიერი გამორიცხული კონტროლის მიზნის და კონტროლის მექანიზმების ჩამონათვალს და გამორიცხვის დასაბუთებას.

მუხლი 10. ორგანიზაციის იუმს-ის დოკუმენტაციის მართვა

1. ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის დოკუმენტაციის უახლესი ვერსიის ხელმისაწვდომობა ყველა უფლებამოსილი პირისთვის, ასევე იუმს-ის დოკუმენტაცის სათანადოდ დაცვა და კონტროლი *(იხ. დანართი № 1, ცმს 27001:2011 თავი 4.3.2.*).

2. ორგანიზაციამ უნდა აწარმოოს ჩანაწერები და უზრუნველყოს მათი მხარდაჭერა იუმს-ის მოთხოვნებთან შესაბამისობისა და ეფექტიანი ფუნქციონირების მიზნით. ჩანაწერები უნდა იყოს სათანადოდ დაცული და კონტროლდებოდეს *(იხ. ცმს 27001:2011 თავი 4.3.3*).

3. ორგანიზაციის იუმს-ის დოკუმენტაცია მოიცავს *(იხ. ცმს 27001:2011 თავი 4.3.1*):

ა) იუმს-ის პოლიტიკას;

ბ) იუმს-ის გავრცელების სფეროს;

გ) იუმს-ის მხარდამჭერ პროცედურებსა და კონტროლებს;

დ) რისკების შეფასების მეთოდოლოგიის აღწერას;

ე) რისკების შეფასების ანგარიშს;

ვ) რისკების მოპყრობის გეგმას (არ არის სავალდებულო პირველ წელს);

ზ) კონტროლის მექანიზმების ეფექტიანობის საზომების აღწერას (არ არის სავალდებულო პირველ წელს);

თ) ჩანაწერებს;

ი) კონტროლის მექანიზმების გამოყენებადობის განაცხადს.

თავი III

ორგანიზაციისთვის მეორე წელს შესასრულებელი მოთხოვნები

მუხლი 11. რისკების მოპყრობის გეგმა

1. ორგანიზაციამ უნდა ჩამოაყალიბოს და დანერგოს რისკების მოპყრობის გეგმა *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.2.ა-გ)*, რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების მართვისათვის საჭირო ქმედებებს ხელმძღვანელობის მხრიდან, რესურსებს *(იხ. დანართი №1, ცმს 27001:2011, თავი 5.2.1)*, პასუხისმგებლობებს და პრიორიტეტებს.

2. ორგანიზაციამ უნდა უზრუნველყოს კონტროლის მიზნების მიღწევა, რაც გულისხმობს სახსრების განაწილებას და პასუხისმგებლობების და როლების განსაზღვრას.

მუხლი 12. ორგანიზაციაში კონტროლის მექანიზმების დანერგვა

ინფორმაციული უსაფრთხოების მიზნების მისაღწევად ორგანიზაცია ვალდებულია:

ა) დანერგოს ამ მოთხოვნის პირველი წლის მე-8 მუხლის მე-5 პუნქტში შერჩეული კონტროლის მექანიზმები;

ბ) კონტროლის მექანიზმების დანერგვისთანავე აწარმოოს მათზე დაკვირვება;

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

მუხლი 13. კონტროლის მექანიზმების ეფექტიანობის საზომების განსაზღვრა

1. ორგანიზაციამ უნდა განსაზღვროს შერჩეული კონტროლის მექანიზმების ან კონტროლის მექანიზმთა ჯგუფის ეფექტიანობის საზომები და დაადგინოს თუ როგორ და ვის მიერ მოხდება ამ საზომების გამოყენება, რათა შეფასდეს კონტროლის მექანიზმების ეფექტიანობა და მიღებული იქნას შედარებადი და განმეორებადი შედეგები *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.2.დ)*.

2. კონტროლის მექანიზმის ეფექტიანობის გაზომვა ხელმძღვანელობას და პერსონალს საშუალებას აძლევს განსაზღვრონ, რამდენად ეფექტიანად იძლევა შერჩეული კონტროლის მექანიზმი კონტროლის მიზნების მიღწევის საშუალებას.

მუხლი 14. ტრენინგები, ცნობიერების ამაღლება და კომპეტენცია

1. ორგანიზაციამ უნდა შეიმუშავოს და განახორციელოს სატრენინგო და ცნობიერების ამაღლების პროგრამები *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.2.ე)*. ორგანიზაციამ უნდა უზრუნველყოს პერსონალის კვალიფიციურობა იუმს-სთან მიმართებაში შემდეგი საკითხების გათვალისწინებით:

ა) იუმს-ში ჩართული პერსონალისთვის აუცილებელი ცოდნის განსაზღვრა;

ბ) ტრენინგების და სხვა ღონისძიებების ჩატარება (მაგ. კომპეტენტური პერსონალის აყვანა) იუმს-ის საჭიროებების დასაკმაყოფილებლად;

გ) სწავლების, ტრენინგის, უნარ-ჩვევების, გამოცდილების და კომპეტენციის შესახებ ჩანაწერების წარმოება.

2. ორგანიზაციამ უნდა უზრუნველყოს, რომ შესაბამისი პერსონალი აცნობიერებს ინფორმაციული უსაფრთხოების ღონისძიებების მნიშვნელოვნებას და მათ მიერ იუმს-ის მიზნების მიღწევაში შეტანილ

წვლილს.

მუხლი 15. იუმს-ის მონიტორინგისთვის საჭირო ქმედებების განსაზღვრა და დანერგვა

ორგანიზაციამ უნდა დანერგოს პროცედურები და სხვა კონტროლის მექანიზმები, რაც საშუალებას მისცემს აღმოაჩინოს უსაფრთხოების შემთხვევები და რეაგირება მოახდინოს ინფორმაციული უსაფრთხოების ინციდენტებზე *(იხ. დანართი №1, 27001:2011, თავი 4.2.2. თ).*

თავი IV

ორგანიზაციისთვის მესამე წელს შესასრულებელი მოთხოვნები

მუხლი 16. მონიტორინგი

1. ორგანიზაციამ უნდა დანერგოს და განახორციელოს მონიტორინგის და განხილვის პროცედურები, ასევე, სხვა კონტროლის მექანიზმები *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.3.ა)*, რომელთა მიზანია:

ა) დამუშავების შედეგებში შეცდომების მყისიერი აღმოჩენა;

ბ) უსაფრთხოების გარღვევის მცდელობების და წარმატებული მცდელობების, აგრეთვე ინციდენტების მყისიერი აღმოჩენა;

გ) მიეცეს ხელმძღვანელობას მსჯელობის საშუალება, თუ რამდენად ეფექტიანად მუშაობს უსაფრთხოების კონკრეტული ღონისძიება;

დ) გამოავლინოს უსაფრთხოების შემთხვევების ინდიკატორების მეშვეობით;

ე) განსაზღვროს, იყო თუ არა გარღვევის მცდელობის აღმოფხვრა ეფექტიანი.

2. ორგანიზაციამ პერიოდულად უნდა განიხილოს იუმს-ის ეფექტიანობა (მათ შორის, იუმს პოლიტიკის და მიზნების, უსაფრთხოების კონტროლის მექანიზმების მიმოხილვა). პერიოდული მიმოხილვის დროს ორგანიზაციამ უნდა გაითვალისწინოს ინფორმაციული უსაფრთხოების აუდიტის შედეგები, ინციდენტები, ეფექტიანობის გაზომვის შედეგები და დაინტერესებული მხარეებისგან მიღებული შემოთავაზებები და უკუკავშირი *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.3.ბ).*

3. ორგანიზაციამ უნდა გაზომოს კონტროლის მექანიზმების ეფექტიანობა უსაფრთხოების მოთხოვნების დაკმაყოფილების დასადასტურებლად *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.3.გ).*

მუხლი 17. რისკების შეფასების გადახედვა

ორგანიზაციამ დაგეგმილი პერიოდულობით უნდა განახორციელოს რისკების შეფასების, ნარჩენი რისკებისა და რისკების მისაღები დონეების გადახედვა *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.3.დ)*, შემდეგი საკითხების გათვალისწინებით:

ა) ორგანიზაციულ-სტრუქტურული ცვლილება;

ბ) ტექნოლოგიური ცვლილება;

გ) ცვლილება საქმიანობის მიზნებსა და პროცესებში;

დ) ახლადაღმოჩენილი საფრთხეები;

ე) დანერგილი კონტროლის მექანიზმების ეფექტიანობის ცვლილება;

ვ) გარე მოვლენები, ისეთი როგორიცაა საკანონმდებლო ცვლილებები;

ზ) შეცვლილი საკონტრაქტო ვალდებულებები და ცვლილებები სოციალურ გარემოში.

მუხლი 18. ორგანიზაციაში იუმს-ის შიდა აუდიტი

1. ორგანიზაცია ვალდებულია ჩაატაროს იუმს-ის აუდიტი *(იხ. დანართი №1, ცმს 27001:2011 თავი 6)* დაგეგმილი პერიოდულობით და დაადგინოს იუმს-ის მიზნები, კონტროლის მექანიზმები, პროცესები და პროცედურები იმის დასადგენად:

ა) შეესაბამება თუ არა სტანდარტის, საკანონმდებლო მოთხოვნებს;

ბ) შეესაბამება თუ არა გამოვლენილ უსაფრთხოების მოთხოვნებს;

გ) ეფექტიანად ხდება თუ არა მისი დანერგვა და მხარდაჭერა;

დ) ფუნქციონირებს თუ არა გეგმის შესაბამისად.

2. ხელმძღვანელობას, რომლის მართვის სფეროში მყოფი საქმიანობაც მოწმდება, ევალება შეუსაბამობების და მათი გამომწვევი მიზეზების აღმოფხვრა. შემდგომი ღონისძიებები გულისხმობს მათ შემოწმებას და შემოწმების შედეგების ანგარიშგებას *(იხ. დანართი №1, ცმს 27001:2011 თავი 8).*

მუხლი 19. ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა

1. ორგანიზაციამ უნდა განახორციელოს იუმს-ის პერიოდული მიმოხილვა, რათა უზრუნველყოფილი იყოს ადეკვატური გავრცელების სფერო და იუმს-ს პროცესის გაუმჯობესებების აღმოჩენა *(იხ. დანართი N 1, ცმს 27001:2011, თავი 7).*

2. ხელმძღვანელობა ვალდებულია აწარმოოს იუმს-ს მიმოხილვა დაგეგმილი პერიოდულობით (სულ მცირე წელიწადში ერთხელ) მუდმივი შესაბამისობის, ადექვატურობისა და ეფექტიანობის უზრუნველსაყოფად. მიმოხილვა უნდა მოიცავდეს გაუმჯობესების გზების მოძიებას და იუმს-ის ცვილებების საჭიროებას, მათ შორის ინფორმაციული უსაფრთხოების პოლიტიკას და მიზნებს.

3. მიმოხილვის შედეგები უნდა იყოს დოკუმენტირებული და ხდებოდეს ჩანაწერების წარმოება *(იხ. დანართი №1, ცმს 27001:2011 თავი 4.3.3*).

მუხლი 20. ინფორმაციული უსაფრთხოების ღონისძიებების გეგმების განახლება

ორგანიზაციამ მონიტორინგის და მიმოხილვის შედეგების გათვალისწინებით უნდა განაახლოს ინფორმაციული უსაფრთხოების ღონისძიებების გეგმები *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.3.ზ).*

მუხლი 21. ორგანიზაციაში იუმს-ის გაუმჯობესება და კომუნიკაცია

ორგანიზაცია ვალდებულია:

ა) იუმს-ში დანერგოს გამოვლენილი გაუმჯობესებები *(იხ. დანართი №1, ცმს 27001:2011, თავი 4.2.4.ა)*;

ბ) განახორციელოს ყველა დაინტერესებული პირის ინფორმირება გატარებული ქმედებების და გაუმჯობესებების თაობაზე დეტალიზაციის შესაბამისი დონის გათვალისწინებით და, საჭიროების შემთხვევაში, შეათანხმოს შემდგომი ნაბიჯები ინფორმაციული უსაფრთხოების მართვის სისტემაზე პასუხისმგებელ პირებთან *(იხ. დანართი № 1, ცმს 27001:2011, თავი 4.2.4.გ;).*

მუხლი 22. იუმს-ის მხარდაჭერა

1. ორგანიზაცია ვალდებულია მუდმივად იზრუნოს იუმს-ის ეფექტიანობის გაუმჯობესებაზე შემდეგი საკითხების გათვალისწინებით:

ა) ინფორმაციული უსაფრთხოების პოლიტიკა და ინფორმაციული უსაფრთხოების მიზნები;

ბ) აუდიტის შედეგები;

გ) მონიტორინგის შედეგად აღმოჩენილი მოვლენების ანალიზი, მაკორექტირებელი და პრევენციული ქმედებები;

დ) ხელმძღვანელობის მიერ იუმს-ის მიმოხილვა *(იხ. დანართი №1, ცმს 27001:2011 თავი 7).*

2. ორგანიზაცია ვალდებულია:

ა) განახორციელოს ცმს 27001:2011-ის 8.2-სა და 8.3-ის თანახმად შესაბამისი მაკორექტირებელი და პრევენციული ქმედებები;

ბ) უზრუნველყოს გაუმჯობესებების შედეგად დასახული მიზნების მიღწევა.